A Theory of Invariants.

By Leonard Eugene Dickson.

General Theory, §§ 1–6.

1. Consider a system S of forms $f_1, .., f_s$ on m variables, where f_i is the general polynomial of degree d_i, having as coefficients arbitrary parameters in any given field F, finite or infinite. Let L be any given group of m-ary linear homogeneous transformations with coefficients in F. The particular systems $S', S'', ..,$ obtained from the general system S by assigning to the coefficients particular sets of values in the field, may be separated into classes C_i under the group L, such that S' and S'' belong to the same class if and only if they are equivalent under L.

We shall employ the term function in Dirichlet's sense of correspondence and shall consider only single-valued functions taking exclusively values in the field F.

Let the function ϕ have one and only one value in field for each of the systems $S', S'', \ldots$ In particular, if, for each i, ϕ has the same value v_i for all the systems in the class C_i, then ϕ is an invariant under the group L.

For a finite field such an invariant is a rational integral function of the coefficients of S, an explicit expression for which is given in § 4. More convenient expressions may be given when S is a special system (§§ 10–18).

2. Let the invariants $I_1, .., I_r$ completely characterize the classes C_i, *i. e.*, each I_k has the same value for two classes only when the latter are identical. Let ϕ be any invariant of the kind defined in § 1. Then ϕ takes one and only one value for each class, while there is one and only one class for each set of values of the I_k. Hence ϕ is a single-valued function of $I_1, .., I_r$, as related.

In particular, let ϕ be a rational integral function of the coefficients of S. Let ϕ be of degree α_{ij} in the coefficient a_{ij}. Then ϕ is completely determined by $N = \Pi(\alpha_{ij}+1)$ distinct* sets of values of the a_{ij} in the field. By means of

* For the $GF[p^n]$, we may set $a_{ij} \leq p^n - 1$.

the resulting N sets (not necessarily distinct) of values of $I_1, .., I_r$, we may construct by a general interpolation formula (§ 3) a polynomial in $I_1, .., I_r$ which takes the same values as ϕ for the N sets. *Hence any rational integral invariant is a rational integral function of* $I_1, .., I_r$.

3. *Interpolation for Any Number of Variables.* We construct a polynomial in $x, y, z, ..,$ which takes prescribed values for a finite number of distinct sets of values of the variables. Consider first the case of two variables. Let x take the distinct values $x_1, .., x_r$. When $x = x_i$, let y take the distinct values $y_{i1}, .., y_{is_i}$. We desire a polynomial $P(x, y)$, which shall take the value v_{ij} when $x = x_i$, $y = y_{ij}$, for each set of subscripts i, j. By any interpolation formula in one variable y, construct for each i a polynomial $Y_i(y)$ which takes the value v_{ij} for $y = y_{ij}$ $(j = 1, .., s_i)$. For example, Lagrange's formula gives

$$Y_i(y) = \sum_{j=1}^{s_i} v_{ij} \prod_{J=1,..,s_i;\ J\neq j} \left(\frac{y - y_{iJ}}{y_{ij} - y_{iJ}}\right). \tag{1}$$

Next, we construct a polynomial P in x which becomes Y_i for $x = x_i$. If we again use Lagrange's formula, we have

$$P(x, y) = \sum_{i=1}^{r} Y_i(y) \prod_{I=1,..,r;\ I\neq i} \left(\frac{x - x_I}{x_i - x_I}\right). \tag{2}$$

When the function (1) is inserted into (2), we obtain the required interpolation formula for two variables. The extension to three or more variables is obvious. Speaking geometrically, we first interpolate for the points in each line parallel to one of the Cartesian axes of coordinates, then for the various lines in a plane parallel to a coordinate plane, etc.

4. An important case is that in which each variable ranges independently over the p^n elements e_i of the Galois field $GF[p^n]$. Then* in (1) the product may be given the form $(y^{p^n} - y)/(e_j - y)$. Thus

$$P(x, y) = \sum_{i,j=1}^{p^n} v_{ij} \frac{(x^{p^n} - x)(y^{p^n} - y)}{(e_i - x)(e_j - y)}. \tag{3'}$$

In general, the integral function obtained from

$$P(x_1, .., x_s) = \sum_{i_1,..,i_s}^{1,..,p^n} v_{i_1,..,i_s} \frac{(x_1^{p^n} - x_1)..(x_s^{p^n} - x_s)}{(e_{i_1} - x_1)..(e_{i_s} - x_s)}, \tag{3}$$

takes the value $v_{i_1,..,i_s}$ for $x_1 = e_{i_1}, .., x_s = e_{i_s}$. Any polynomial, of degree $\leq p^n - 1$ in each x, which takes these values v is identical with P.

* Cf. *Annals of Mathematics*, 1897, p. 69.

For a system S of forms in a finite field the investigation of invariants, which take one and but one value in the field for each set of values of the coefficients, may therefore be restricted to polynomials in the coefficients. The *characteristic** invariant I_k for the class C_k is that invariant which has the value unity for the class C_k and the value zero for the remaining classes. Let $a_1, \ldots, a_s$ be the coefficients in the system S; $a_1^{(k)}, \ldots, a_s^{(k)}$ the coefficients in a system of forms in the class C_k. Then by (3),

$$I_k = \sum_{a_1^{(k)}, \ldots, a_s^{(k)}} \prod_{j=1}^{s} \frac{a_j^{p^n} - a_j}{a_j^{(k)} - a_j}. \tag{4}$$

In particular, for the class C_0, composed of the system of forms with all coefficients zero, the characteristic invariant is

$$I_0 = \prod_{j=1}^{s} (1 - a_j^{p^n - 1}). \tag{4'}$$

From the definition of the I_k or from their expressions (4), we have

$$I_k^2 = I_k, \quad I_k I_l = 0 \ (l \neq k), \quad \sum_{k=0}^{f-1} I_k = 1, \tag{5}$$

where f denotes the number (necessarily finite) of the classes.

Any invariant I takes certain values $v_0, \ldots, v_{f-1}$ for the classes $C_0, \ldots, C_{f-1}$, so that $I = \Sigma v_k I_k$. *Any invariant can be expressed in one and but one way as a linear homogeneous function of the characteristic invariants. The number of linearly independent invariants equals the number of classes.*

The fact that any invariant is a linear function of the I_k also follows from (5) and the general theorem in § 2, since the present set of I_k is a special case of the set there discussed.

5. When the group L is the group G of all m-ary linear homogeneous transformations in the field F, the invariants, defined in § 1, are *absolute* invariants of the system S. When L is the group G_1 of all the transformations of determinant unity, those invariants of G_1 which are multiplied by Δ^w under any transformation of determinant Δ are *relative* invariants of *weight* w of the system S.

The theory of the characteristic invariants enables us to prove (*Transactions, l. c.*) that *when F is the $GF[p^n]$, the number of linearly independent invariants, relative and absolute, equals the number of classes under the group G_1.*

* *Transactions Amer. Math. Soc.*, Vol. X (1909), p. 126. The existence of the invariants was there established, but not the explicit formulæ (3), (4).

In the special systems investigated below, we do not presuppose this result, but obtain a direct verification of it.

6. In the investigation of the invariants of a system of forms in a field F under a group L, the chief aim is the determination of a fundamental system of independent invariants* (all invariants being single-valued functions of these) and a complete set of independent relations between them. A practical method of determining these relations for the case of a finite field may be based upon the knowledge of a complete set of linearly independent invariants. As we shall usually not go to the trouble (in general very great) to determine† the characteristic invariants, we propose the following procedure‡ for the determination of a complete set of linearly independent invariants, which establishes automatically their linear independence.

Let the classes be separated into sets $K_1, K_2, .., K_l$ (in practice by specifying the ranges of certain parameters) and let there be associated with K_i a set V_i of linearly independent§ invariants, in number equal to the number of classes in K_i, and such that every invariant in the set V_i vanishes for all sets K_j $(j > i)$. The aggregate of the invariants in the sets V_i constitutes a complete system of linearly independent invariants. Indeed, their number is the total number of classes, while any linear relation has its coefficients all zero, as shown by employing in turn the classes in $K_l, K_{l-1}, .., K_1$. For instance, for the classes in K_l, the invariants in $V_1, .., V_{l-1}$ vanish, and those in V_l are linearly independent.

In particular, if L is the group G_1 (§ 5), we obtain a complete set of linearly independent relative and absolute invariants, when the chosen invariants of the sets V_i are of that kind.

Field || *C of all Real and Complex Numbers.*

7. Consider a single quadratic form on m variables. Denote its determinant by D. Within the group G_1, a complete set of canonical types is

$$Dx_1^2 + x_2^2 + .. + x_m^2 \ (D \neq 0), \quad x_1^2 + .. + x_i^2 \ (i = 1, .., m-1), \quad 0.$$

---

* To be chosen on the basis of their expressing fundamental properties of the system of forms, rather than the simplicity of their expressions or the smallness of their number.

† More explicitly than by the general expression (4).

‡ First employed in my paper on the modular invariants of the general system of q linear forms in m variables, *Proc. Lond. Math. Soc.*, 1909.

§ Tested by employing the classes in K_i alone.

|| The discussion in §§ 7–9 applies also to the infinite field F_p given by the aggregate of the Galois fields of orders p^n, $n = 1, 2, 3, ...$, provided $p < m$ (also to certain fields contained in F_p).

The classes are completely characterized by the invariants D and r, where r is the rank of the matrix of the form. Thus D and r form a fundamental system of invariants. A complete set of independent relations is

$$r(r-1)\,..\,(r-m)=0, \quad rD=mD.$$

A polynomial in D and r therefore equals the sum of a polynomial in D and a polynomial in r. Thus (§ 2) the only rational integral invariants are the polynomials in D. The characteristic invariant for $x_1^2+\,..\,+x_i^2\,(i<m)$, including 0 for $i=0$, is

$$\Pi\binom{r-t}{i-t} \quad (t=0,\ 1,\ ..,\ m;\ t\neq i).$$

8. A binary cubic form in C can be transformed within G_1 into one of the canonical types x^3, $xy(x+ry)$, 0, where r is a particular square root of the discriminant D. The corresponding classes may be designated T, C_D, V. Let m be the function of the coefficients which specifies the maximum multiplicity of a linear factor, viz., $m=3,\ 2,\ 1,\ 0$ for classes T, C_0, $C_D\,(D\neq 0)$, V, respectively. Hence D and m form a fundamental system of invariants. A complete set of independent relations is

$$m(m-1)(m-2)(m-3)=0, \quad mD=D.$$

Thus $P(D, m)=P_1(D)+P_2(m)$, where the P's denote polynomials. Hence (§ 2) the only rational invariants are $P_1(D)$. The characteristic invariants for T, C_0, V are

$$\tfrac{1}{6}m(m-1)(m-2),\ -\tfrac{1}{2}m(m-1)(m-3),\ -\tfrac{1}{6}(m-1)(m-2)(m-3).$$

9. For the field C we consider a pair of binary quadratic forms with the determinants a, b, bilinear invariant θ, and resultant R (§ 13).

If $R\neq 0$, the family has two independent unary forms, which become multiples of x^2 and y^2 under a transformation of G_1. Then

$$q_1=a_0x^2+a_2y^2, \quad q_2=b_0x^2+b_2y^2, \quad R=-(a_0b_2-a_2b_0)^2\neq 0.$$

Applying $(y, -x)$ if necessary, we may set $a_0\neq 0$. Applying $(\rho x, \rho^{-1}y)$, where $\rho^2=a_0^{-1}$, we obtain a similar pair with $a_0=1$, viz.,

$$Q_1=x^2+ay^2, \quad Q_2=B_0x^2+B_2y^2, \quad B_0B_2=b, \quad B_2+aB_0=\theta.$$

If $a=0$, then $\theta^2=-R$, $\theta\neq 0$, $B_2=\theta$, $B_0=b/\theta$. If $a\neq 0$,

$$B_0=(\theta\pm\sqrt{-R})/(2a), \quad B_2=(\theta\mp\sqrt{-R})/2.$$

But the two resulting pairs of forms are interchanged by $(a^{\frac{1}{2}}y, -a^{-\frac{1}{2}}x)$. Hence the invariants a, b, θ completely characterize the classes with $R \neq 0$ under G_1.

If the rank r_1 of q_1 is zero, so that $q_1 \equiv 0$, the classes are characterized by $r_1 = 0$ and the values of b, r_2 (§ 7). For use in characterizing* the classes in which $q_1 \not\equiv 0$, $q_2 = cq_1$, let $M = c$ in that case, but $M = 0$ if $q_1 \equiv 0$ or if $q_1 \not\equiv 0$ and q_2 is not a multiple of q_1. According to the definition in § 1, M is an invariant. We may also define M by means of the pencil $\lambda q_1 + \mu q_2$, λ and μ being arbitrary variables; if the functions $\lambda a_i + \mu b_i$ have a common divisor of the form $\lambda + c\mu$, we take $M = c$; in the contrary case, we take $M = 0$.

It remains to consider the case $R = 0$, $M = 0$, $r_1 > 0$, $r_2 > 0$, so that neither q_1 nor q_2 vanishes identically, and q_2 is not a multiple of q_1. Then

$$d = a_0b_1 - a_1b_0, \quad e = a_0b_2 - a_2b_0, \quad f = a_1b_2 - a_2b_1 \tag{6}$$

are not all zero, viz., the Jacobian of q_1 and q_2 is not identically zero. We have the relations

$$R = 4df - e^2, \quad a_0f - a_1e + a_2d = 0. \tag{7}$$

Multiply (7_1) by a_0^2 and eliminate f by (7_2). Then since $R = 0$,

$$\delta^2 = -4ad^2, \quad \delta \equiv a_0e - 2a_1d. \tag{8}$$

For the present case, a and b are not both zero.

(i) $a \neq 0$. First, let $a_0 \neq 0$. Then $d \neq 0$. Let $r = \delta/(2d)$. Then r is a particular square-root of $-a$. Applying the transformation of determinant unity,

$$x = \frac{r + a_1}{a_0}X + \frac{r - a_1}{2r}Y, \quad y = -X + \frac{a_0}{2r}Y, \tag{9}$$

we get (since $r^2 = -a$)

$$q_1 = 2rXY, \quad q_2 = \beta_0X^2 - r^{-1}\theta XY + \beta_2Y^2, \tag{10}$$

$$\beta_0 = (\delta - 2rd)/a_0^2, \quad \beta_2 = (\delta + 2rd)/(4r^2). \tag{11}$$

Inserting the special value of r, we have $\beta_0 = 0$, $\beta_2 \neq 0$. Applying a transformation (ρ, ρ^{-1}), we obtain

$$Q_1 = 2rXY, \quad Q_2 = -r^{-1}\theta XY + Y^2. \tag{12}$$

Next, let $a_0 = 0$, so that $a_1 \neq 0$. Eliminating e from (7), we get

$$dk = 0, \quad k \equiv 4a_1^2f - a_2^2d.$$

The factors d, k are not both zero. If $d = 0$, so that $b_0 = 0$, the transformation of determinant unity

$$x = X - \tfrac{1}{2}a_1^{-1}a_2Y, \quad y = Y \tag{13}$$

* It suffices to employ M alone if $M \neq 0$, but $r_1 > 0$, a, $r_2 = 0$, if $M = 0$.

replaces q_1, q_2 by (10) with $r = a_1$, $\beta_0 = b_0$, $\beta_2 = k/(4a_1^3) \neq 0$. If $d \neq 0$, so that $k = 0$, the transformation

$$x = \tfrac{1}{2} a_1^{-1} a_2 X + Y, \quad y = -X$$

replaces q_1, q_2 by (10) with $r = -a_1$, $\beta_0 = k/(4a_1^3)$, $\beta_2 = b_0 \neq 0$. In the last two cases we obtain (12) with $r = a_1$ and $-a_1$, respectively.

In every case we have obtained the canonical type (12) in which r is a particular square-root of the invariant $-a$. No transformation of G_1 replaces (12) to a like pair with the parameter $-r$. The additional invariant V_a necessary to characterize the classes may be defined by its values as follows: If $R \neq 0$, or $M \neq 0$, or $r_2 = 0$, or $a = 0$, set $V_a = 0$. If $R = M = 0$, $r_2 > 0$, $a \neq 0$, set

$$V_a = \delta/(2d) \text{ for } a_0 \neq 0, \quad V_a = a_1 \text{ for } a_0 = d = 0, \quad V_a = -a_1 \text{ for } a_0 = 0, \ d \neq 0.$$

Since V_a has the same value for all sets of forms in a class, it is an invariant. For the corresponding rational integral invariant in a finite field, see § 14.

(ii) $b \neq 0$. We employ the invariant V_b derived from V_a by interchanging the a's and b's. By modifying our definition of V_a when $a = 0$, we could make a single invariant cover both cases $a \neq 0$ and $a = 0$, $b \neq 0$.

We have now shown that a complete system of invariants is given by

$$a, \ b, \ \theta, \ r_1, \ r_2, \ M, \ V_a, \ V_b. \tag{14}$$

Invariants of Two Binary Quadratic Forms in the $GF[2^n]$.

10. Since the modulus is 2, the forms are designated

$$q_1 = a_0 x^2 + a_1 xy + a_2 y^2, \quad q_2 = b_0 x^2 + b_1 xy + b_2 y^2. \tag{15}$$

A single form q_1 has the invariants,* the third being (4′),

$$a_1, \quad H_a = \chi(a_0 a_1^e a_2), \quad I_a = \prod_{i=0,1,2} (1 - a_i^m), \tag{16}$$

where $e = 2^n - 3$ if $n > 1$, $e = 1$ if $n = 1$, while

$$m = 2^n - 1, \quad \chi(s) = \sum_{i=0}^{n-1} s^{2^i}.$$

The necessary and sufficient condition that q_1 be irreducible in the field is $H_a = 1$; that it be the product of two distinct linear factors, $H_a = 0$, $a_1 \neq 0$; that it be a perfect square, $a_1 = I_a = 0$; that it vanish identically, $I_a = 1$ Within the group G_1, the corresponding canonical forms are

$$Q_1 = a_1^2 x^2 + a_1 xy + cy^2, \quad a_1 xy, \quad x^2, \quad 0, \tag{17}$$

* Concerning the invariants here employed, see AMERICAN JOURNAL OF MATHEMATICS, Vol. XXXI (1909), pp. 109, 115. This paper is cited henceforth as *A. J.*

where $a_1 \neq 0$ and c is a particular solution of $\chi(c) = 1$. Hence, by § 2, the three invariants (16) form a fundamental system of invariants of q_1.

When q_1 is transformed within G_1 into one of the types (17), let q_2 become

$$Q_2 = B_0 x^2 + b_1 xy + B_2 y^2.$$

For (17_1) it suffices to normalize

$$Q_2 - a_1^{-1} b_1 Q_1 = l^2, \quad l \equiv rx + sy.$$

For the eliminant of Q_1, l and the resultant of q_1, q_2, we have

$$E = a_1^2 s^2 + a_1 rs + cr^2, \quad R = E^2.$$

If $E = 0$, then $r = s = 0$ by the irreducibility of Q_1, so that the forms are already in their canonical form (I). If $E \neq 0$,

$$\begin{pmatrix} ksa_1 & krca_1^{-1} \\ kra_1 & k(r + sa_1) \end{pmatrix}, \quad k \equiv E^{-\frac{1}{2}}$$

is an automorph of Q_1, has determinant unity, and replaces l by $E^{\frac{1}{2}} a_1^{-1} y$. Hence, if q_1 is irreducible, the canonical type is

(I) $\quad Q_1 = a_1^2 x^2 + a_1 xy + cy^2, \quad Q_2 = a_1^{-1} b_1 Q_1 + a_1^{-2} R^{\frac{1}{2}} y^2 \quad (a_1 \neq 0).$

As in *A. J.*, § 18, § 19 (with $k = 1$), the remaining canonical types are

(II), (III) $\quad Q_1 = a_1 xy, \quad Q_2 = x^2 + b_1 xy + a_1^{-2} Ry^2$, or $b_1 xy \quad (a_1 \neq 0)$;

(IV) $\quad Q_1 = x^2, \quad Q_2 = b_1^2 cR^{-\frac{1}{2}} x^2 + b_1 xy + R^{\frac{1}{2}} y^2 \quad (b_1 R \neq 0)$;

(V), (VI) $\quad Q_1 = x^2, \quad Q_2 = b_1 xy + R^{\frac{1}{2}} y^2$ (b_1, R not both 0), or $b_0 x^2$;

(VII)–(X) $\quad Q_1 = 0, \quad Q_2 = b_1^2 x^2 + b_1 xy + cy^2, \ b_1 xy, \ x^2, \ 0 \quad (b_1 \neq 0).$

To construct the additional invariant required by the type VI, we may proceed as with M in § 9, or as follows. The relation

$$I_{a+kb} = I_a + I_a (I_b + 1) k^m + \sum_{r=1}^{m} k^r Z_r \quad (k^{m+1} \equiv k)$$

defines certain absolute invariants Z_r. But $Z_r = Z_1^r$, as shown in *A. J.*, § 21; while Z_1 has the following characteristic properties: If q_1 is not identically zero, $Z_1 = t$ when $q_2 \equiv tq_1$, $Z_1 = 0$ when q_2 is not a constant multiple of q_1; if $q_1 \equiv 0$, then $Z_1 = 0$. Thus $Z_1 = (1 - R^m) a_1^{-1} b_1$ for type I, $a_1^{-1} b_1$ for III, b_0 for VI, zero for the remaining types.

We thus employ Z_1 to differentiate the types VI from each other, and type II with $R = 0$, $b_1 \neq 0$ from type III with $b_1 \neq 0$. The invariants

$$a_1, \ H_a, \ I_a, \ b_1, \ H_b, \ I_b, \ R, \ Z_1 \tag{18}$$

completely characterize the types I, .., X and hence (§ 2) *form a fundamental system of invariants of forms* (15) *in the* $GF[2^n]$.

These eight invariants are independent (*A. J.*, § 23). By employing invariants whose interpretation is not so immediate, we may obtain (*A. J.*, § 32) a fundamental system of six invariants (four if $n = 1$).

11. THEOREM. *The $2^{3n+1} + 2^{2n}$ invariants* in the accompanying table form a complete set of linearly independent invariants of two binary quadratic forms in the $GF[2^n]$.*

The following table is arranged according to the principle in § 6. The number N of canonical types specified in any line equals the number of invariants in that line, the linear independence of the latter being readily established by inserting the values of the invariants for the forms in that line. The linear independence of all the invariants then follows from the fact that each invariant vanishes for all the types in the later lines of the table.

PAIRS OF FORMS.	INVARIANTS.	NUMBER.
I, $H_b = 1$	$H_a H_b a_1^i b_1^j R^e$	$m^2 2^{n-1}$
I, $H_b = 0$, $b_1 \neq 0$	$H_a a_1^i b_1^{j+1} R^e$	$m^2 2^{n-1}$
I, $b_1 = 0$	$H_a a_1^i R^j$, $H_a a_1^i I_b$	$m\,2^n$
III	$a_1^{i+1} I_b$, $a_1^{i+1} Z_1$, $a_1^i b_1^j Z_1 (j > 0)$	$m\,2^n$
II, $H_b = 1$	$H_b a_1^{i+1} b_1^j R^e$	$m^2 2^{n-1}$
II, $H_b = 0$, $b_1 \neq 0$	$a_1^{i+1} b_1^{j+1} R^e$	$m^2 2^{n-1}$
II, $b_1 = 0$	$a_1^{i+1} R^j$, $a_1^{i+1} R^m$	$m\,2^n$
VII	$I_a b_1^i H_b$	m
VIII	$I_a b_1^{i+1}$	m
X	$I_a I_b$	1
IX	I_a	1
IV	$H_b b_1^i R^j$	m^2
V, $R \neq 0$	$b_1^i R^{j+1}$, $b_1^m R^{j+1}$	$m\,2^n$
V, $R = 0$	b_1^{i+1}	m
VI	I_b, Z_1^j	2^n

Throughout the table the exponents have the ranges

$$i, j = 0, 1, \ldots, m - 1;\quad e = 0, 1, \ldots, 2^{n-1} - 1.$$

* Identical with the set (82) of *A. J.*, § 28, there proved complete for $n \leq 3$. For $n = 1$, we may delete $a_1 Z_1$ from the fourth line of the table and insert Z_1, in view of (69), *A. J.*

On account of the complexity of the expressions for H_b, we have made three subdivisions for types I and II. Since $\chi(c)=1$, $\chi^2=\chi$, we have for I,

$$H_b=\chi(cb_1^m)+\chi(a_1^{-1}b_1^{2^n-2}R^{1/2})=b_1^m+\chi(a_1^{-2}b_1^{2^n-3}R),$$

the final term being also the value of H_b for type II. Hence in lines 1, 2, 5, 6 of the table, R satisfies an equation of degree 2^{n-1}.

Relations (68)–(73) of *A. J.*, § 25, together with $b_1Z_1=a_1Z_1$ for $n=1$, enable us to express any product of the invariants (18) as a linear function of those in the table.

One Binary Quadratic Form in the $GF[p^n]$, $p>2$.

12. For a single form in the $GF[p^n]$, $p>2$,

$$q_1=a_0x^2+2a_1xy+a_2y^2 \quad (a=a_0a_2-a_1^2), \tag{19}$$

the canonical types within the group G_1 are

$$x^2+ay^2 \ (a\neq 0),\ x^2,\ \nu_1x^2,\ 0 \quad (\nu_1 \text{ a fixed not-square}), \tag{20}$$

according as respectively $a\neq 0$, $-Q=$ square, $-Q=$ not-square, or $a=Q=0$, where Q denotes the absolute invariant (*A. J.*, § 7):

$$Q=(a_0^\tau+a_2^\tau)\{\sum_{i=0}^{\tau}a_0^ia_2^ia_1^{2\tau-2i}-1\} \quad [\tau=\tfrac{1}{2}(p^n-1)]. \tag{21}$$

Hence a and Q form a fundamental system (§ 2). The identically vanishing type may be characterized by $I=1$, where

$$I=1-a^{2\tau}-Q^2=(1-a_0^{2\tau})(1-a_1^{2\tau})(1-a_2^{2\tau}). \tag{22}$$

A complete set of linearly independent invariants is (§ 6)

$$a^i \ (i=1,\ldots,2\tau),\ Q,\ Q^2,\ 1;$$

any relation between them follows from

$$a^{2\tau+1}=a, \quad aQ=0, \quad Q^3=Q.$$

The last two are proved by multiplying (22) by a and Q, respectively.

Two Binary Quadratic Forms in the $GF[p^n]$, $p>2$, §§ 13–17.

13. Consider a pair of forms defined by (19) and

$$q_2=b_0x^2+2b_1xy+b_2y^2 \quad (b=b_0b_2-b_1^2). \tag{23}$$

They have the simultaneous invariant θ and resultant R:

$$\theta=a_0b_2-2a_1b_1+a_2b_0, \quad R=4ab-\theta^2. \tag{24}$$

Invariants (21) and (22) will now be designated Q_a and I_a. For q_2 we have invariants Q_b and I_b. We define absolute invariants K_i by

$$Q_{a+kb} = Q_a + k^r Q_b + \sum_{i=1}^{2r} k^i K_i \quad (k^{2r+1} \equiv k). \tag{25}$$

The values of certain K_i for various types are given in *A. J.*, §§ 8–11.

14. First, let $-a$ be a square $\neq 0$ in the field. For $a_0 \neq 0$, let r be a particular element for which $r^2 = -a$, and employ formulae (9)–(11). For $a_0 = 0$, set $r = a_1$, and employ (13). In either case, we reach type (10). Within the group G_1, a pair (10) is transformed into a similar pair only by $(\rho X, \rho^{-1} Y)$, whence r, β_0^τ, β_2^τ are unaltered, and by $(\rho Y, -\rho^{-1} X)$, whence r is changed in sign and β_0^τ, β_2^τ interchanged. In each case, $t = r(\beta_0^\tau - \beta_2^\tau)$ is unaltered. We therefore seek an invariant V_a of the general pair of forms such that $V_a = 0$ when $-a$ is zero or a not-square, and $V_a = t$ when $-a = r^2$. We thus set

$$V_a = \tfrac{1}{2}\{1 + (-a)^r\} W. \tag{26}$$

First, let the coefficients be such that $-a$ is the square of an element $r \neq 0$. Then $V_a = W$. For $a_0 \neq 0$, we may employ (11) and get $t = F$,

$$F = r\{(\delta - 2rd)^r - (\delta + 2rd)^r\}. \tag{27}$$

Since F involves only even powers of r, it equals a polynomial in the original coefficients. For $a_0 = 0$, we apply (13) and get $t = L$,

$$L = a_1\{b_0^\tau - (a_2^2 b_0 - 4 a_1 a_2 b_1 + 4 a_1^2 b_2)^\tau\}.$$

For any a_0, $W \equiv F + M(1 - a_0^{2r})$. Set $a_0 = 0$; then $L = F_1 + M$, where F_1 is the value $a_1 b_0^\tau$ of F for $a_0 = 0$. Hence

$$W \equiv F - a_1(a_2^2 b_0 - 4 a_1 a_2 b_1 + 4 a_1^2 b_2)^r (1 - a_0^{2r}). \tag{28}$$

Next, let $a = 0$. Then $F = 0$, $W^2 = 0$, since

$$a_1^2(1 - a_0^{2r}) = (a_1^2 - a_0 a_2)(1 - a_0^{2r}).$$

Hence the invariant V_a with the prescribed values is given by (26)–(28). Its weight is 1. In particular, for $p^n = 3$ and $p^n = 5$, we obtain, respectively,

$$V_a = b_1(a_1^2 + a_0 a_2)(a_2 - a_0) + a_1 b_2(a_0^2 - 1) + a_1 b_0(1 - a_2^2), \tag{29}$$

$$V_a = b_0^2 a_1(1 - a_2^4) + b_2^2 a_1(a_0^4 - 1) + (b_1^2 - 2 b_0 b_2)(a_1^2 - 2 a_0 a_2) a_1(a_0^2 - a_2^2) + b_1 b_2 P - b_1 b_0 P', \tag{30}$$

where

$$P = 2 a_1^4 a_2(1 - a_0^4) - a_0^3 a(1 + a^2) = 2 a_1^4 a_2 + 2 a_0^3 a_1^2 - 2 a_0 a_1^2 a_2^2 - a_0^2 a_2^3 - a_0^4 a_2, \tag{31}$$

while P' is derived from P by permuting a_0 with a_2 and changing the sign of a_1. By inspection, (29) and (30) are unaltered by $(y, -x)$.

The pair (10) may be transformed by (ρ, ρ^{-1}) into a pair with

$$\beta_0 = 1 \text{ or } \nu_1; \quad \beta_0 = 0, \quad \beta_2 = 0, 1, \nu_1 \quad (\nu_1 \text{ a fixed not-square}). \tag{32}$$

The resulting types are differentiated by the invariants

$$a = -r^2, \quad b = \beta_0\beta_2 + \tfrac{1}{4}a^{-1}\theta^2, \quad \theta, \quad K_\tau = \beta_0^\tau + \beta_2^\tau, \quad V_a = r(\beta_0^\tau - \beta_2^\tau). \tag{33}$$

15. Next, let $a = 0$, $I_a = 0$, so that q_1 is equivalent under G_1 with a_0x^2, where $a_0 = 1$ or ν_1 according to the value of the invariant $Q_a = -a_0^\tau$. Within G_1 an automorph of q_1 transforms q_2 into

$$\theta^{-1}a_0bx^2 + a_0^{-1}\theta y^2 \ (\theta \neq 0), \quad 2a_0^{-\tau}V_bxy \ (\theta = 0, b \neq 0), \quad 2a_0^{1-\tau}K_1x^2 \ (\theta = b = 0), \tag{34}$$

in which V_b is derived from V_a (§ 14) by interchanging the a's and b's.

If $I_a = 1$, so that $q_1 \equiv 0$, invariants b and Q_b characterize the types q_2.

16. Finally, let $-a$ be a not-square ν. Within the group G_1, the pair q_1, q_2 can be transformed into

$$q_1' = x^2 - \nu y^2, \quad q_2' = ex^2 + 2fxy + gy^2, \tag{35}$$

$$\nu = -a, \quad g - e\nu = \theta, \quad eg - f^2 = b. \tag{36}$$

We enlarge the $GF[p^n]$ to the $GF[p^{2n}]$ by adjoining a root of

$$\varepsilon^2 = \nu. \tag{37}$$

By the transformation of determinant unity,

$$X = (x - \varepsilon y)/(2\varepsilon), \quad Y = x + \varepsilon y, \tag{38}$$

$$x = \varepsilon X + \tfrac{1}{2}Y, \quad y = -X + \tfrac{1}{2}\varepsilon\nu^{-1}Y, \tag{38'}$$

the pair (35) becomes

$$Q_1 = 2\varepsilon XY, \quad Q_2 = \varkappa X^2 - \nu^{-1}\theta\varepsilon XY + \sigma Y^2, \tag{39}$$

$$\varkappa = k - 2f\varepsilon, \quad \sigma = (k + 2f\varepsilon)/(4\nu), \quad k = g + e\nu. \tag{40}$$

The only automorphs of determinant unity of Q_1 are

$$X' = \lambda X, \quad Y' = \lambda^{-1}Y. \tag{41}$$

The corresponding transformation T on the variables x, y has its coefficients in the $GF[p^n]$ if and only if $\lambda^{p^n} = \lambda^{-1}$, as follows from the fact that Y is the product of -2ε and the function conjugate to X with respect to the $GF[p^n]$. A direct verification follows from

$$T = \begin{pmatrix} \alpha & \nu\gamma \\ \gamma & \alpha \end{pmatrix}, \quad \alpha = \tfrac{1}{2}(\lambda^{-1} + \lambda), \quad \gamma = \tfrac{1}{2}\nu^{-1}\varepsilon(\lambda^{-1} - \lambda), \quad \varepsilon^{p^n} = -\varepsilon,$$

whence $\lambda = \alpha - \gamma\varepsilon$, $\lambda^{-1} = \alpha + \gamma\varepsilon$, $\lambda^{p^n} = \lambda^{-1}$. The equation

$$\lambda^{p^n+1} = 1 \tag{42}$$

has $p^n + 1$ solutions in the $GF[p^{2n}]$. By (40)

$$\sigma = x^{p^n}/(4\nu), \quad x^{p^n+1} = k^2 - 4\nu f^2 = \theta^2 + 4\nu b = -R. \tag{43}$$

If $R = 0$, then $x = 0$, $k = f = 0$, $q_2' = -\frac{1}{2}\nu^{-1}\theta q_1'$.

Henceforth, let $R \neq 0$. By (43), there are $p^n + 1$ pairs of forms (39). Since $x \neq 0$, (41) is an automorph of Q_2 only when $\lambda^2 = 1$. Hence the pairs of forms (39) fall into two sets each containing $\frac{1}{2}(p^n + 1)$ pairs equivalent under transformations (41), satisfying (42). *For given values of the invariants* ν, b, θ, *with* $R \neq 0$, *the pairs* (35) *fall into two non-equivalent sets under* G_1; *the sets are differentiated by the two square roots of* $-R$ *in the* $GF[p^{2n}]$.

To prove the last statement, set $j = \frac{1}{2}(p^n + 1)$. Under transformation (41), subject to (42), the pair (39) is replaced by a pair with $x' = x\mu$, where $\mu = \lambda^2$ is a root of $\mu^j = 1$. Hence we may restrict x to two values x_1, x_2, such that x_1^j and x_2^j are the two square roots of $-R$.

We proceed to the construction of an invariant Ω of the general pair of forms q_1, q_2 in the $GF[p^n]$, $p > 2$, which will differentiate the two sets just mentioned. To this end, we first determine a non-vanishing of multiple of x^j which is expressible rationally in terms of the coefficients of (35). Since 4 is a square and ν a not-square, $(4\nu)^j = -4\nu$. Hence, by (43),

$$x^j \pm 4\nu\sigma^j = x^j[1 \mp (-R)^\tau], \quad \tau = \tfrac{1}{2}(p^n - 1). \tag{44}$$

According as $-R$ is a not-square or a square in the $GF[p^n]$, we employ the upper or lower signs in (44) and see that the non-vanishing functions

$$U_1 = \varepsilon\{(k - 2f\varepsilon)^j - (k + 2f\varepsilon)^j\}, \quad U_2 = (k - 2f\varepsilon)^j + (k + 2f\varepsilon)^j \tag{45}$$

equal polynomials in ν, e, f, g, which are unaltered by every transformation of determinant unity which replaces (35) by a like pair. Set *

$$\Omega_1 = \tfrac{1}{2}[1-(-a)^\tau]W_1, \quad \Omega_2 = \tfrac{1}{2}[1-(-a)^\tau](-a)^{2\tau}W_2, \tag{46}$$

in which W_i is to be determined so that it shall equal U_i when the general pair of forms becomes (35). Now $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ will replace $x^2 - \nu y^2$ by (19), with $a = -\nu$, and will have determinant unity if

$$\alpha^2 - \nu\gamma^2 = a_0, \quad \beta = (a_1\alpha + \nu\gamma)/a_0, \quad \delta = (\alpha + a_1\gamma)/a_0.$$

* Whence $\Omega_i = 0$ if $-a$ is a square $\neq 0$. For $a = 0$, $W_1 = 0$, $W_2 \neq 0$; hence in Ω_2 we insert the factor a power of $-a$.

The inverse $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ replaces (19) by $x^2 - \nu y^2$, and (23) by q_2' with

$$f = a_0^{-2}(sd - \alpha\gamma t), \quad k = a_0^{-2}(st - 4\nu\alpha\gamma d), \quad t \equiv a_0\theta + 2\nu b_0, \quad s \equiv \alpha^2 + \nu\gamma^2,$$

with d given by (6). Inserting the values of f, k, $\nu = -a$, $e = (k-\theta)/(2\nu)$ into (45), we have the required functions W_i. The resulting forms have the disadvantage that they contain the auxiliary quantities α, γ. For small values of p^n we may effect the expansions, apply $\alpha^2 - \nu\gamma^2 = a_0$, and obtain functions free of α, γ. We shall, however, make use of a different method of attack.

According as a_0 is a square h^2 or a not-square νh^2, we apply

$$S = \begin{pmatrix} h^{-1}, & -a_1 h^{-1} \\ 0, & h \end{pmatrix}, \quad N = \begin{pmatrix} a_1 \nu^{-1} h^{-1}, & h^{-1} \\ -h, & 0 \end{pmatrix}$$

to the general pair of forms (19), (23). For $a_0 = h^2$, we obtain (35), with

$$e = b_0/a_0, \quad f = (a_0 b_1 - a_1 b_0)/a_0, \quad g = a_0 b_2 - 2a_1 b_1 + a_1^2 b_0/a_0. \tag{47}$$

For $a_0 = \nu h^2$, we get

$$-x^2 + \nu y^2, \quad \nu^{-1} g x^2 - 2fxy + \nu e y^2. \tag{48}$$

To the latter we apply transformation (38′) and obtain

$$-2\varepsilon XY, \quad \varkappa^{p^n} X^2 + \nu^{-1}\theta\varepsilon XY + \sigma^{p^n} Y^2, \tag{49}$$

each coefficient being conjugate with the corresponding coefficient in (39). The only transformations of determinant unity multiplying XY by -1 are

$$L = (\mu Y, \ -\mu^{-1} X). \tag{50}$$

By a discussion similar to that for (41), we see that L corresponds to a transformation (56) on x, y with coefficients in the $GF[p^n]$ if and only if

$$\mu^{p^n+1} = \frac{1}{4\nu}. \tag{51}$$

Applying transformation L to the pair (49), we obtain

$$2\varepsilon XY, \quad \varkappa_1 X^2 - \nu^{-1}\theta\varepsilon XY + \sigma_1 Y^2, \quad \varkappa_1 = \sigma^{p^n}/\mu^2, \quad \sigma_1 = \mu^2 \varkappa^{p^n}.$$

As noted above, $(4\nu)^j = -4\nu$, so that by (43) and (51),

$$\varkappa_1^j = -\varkappa^j, \quad \sigma_1^j = -\sigma^j.$$

Hence by (44) and (45), the functions U_i for the pair (48) are the negatives of the functions U_i for the pair (35), subject to (47). Now $a_0^\gamma = +$ or -1 in the respective cases. Hence in each case the desired function W_i is a_0^γ times the function obtained from U_i, in (45), by inserting the values of k and f given by (47), viz.,

$$k = \theta + 2e\nu = \theta - 2ab_0/a_0.$$

Expanding the binomials and replacing ε^2 by $-a$, we get

$$\left.\begin{aligned} \Omega_1 &= a_0^{2r-1}[(-a)^r - 1]\sum_{s=1}^{(j+1)/2} C_{2s-1}^j (-a)^s (2d)^{2s-1} l^{j-2s+1}, \\ \Omega_2 &= a_0^{2r-1}[(-a)^{2r} - (-a)^r]\sum_{s=0}^{j/2} C_{2s}^j (-a)^s (2d)^{2s} l^{j-2s}, \\ d &= a_0 b_1 - a_1 b_0, \quad l = a_0\theta - 2ab_0. \end{aligned}\right\} \tag{52}$$

Invariant Ω_1 is of weight 3, Ω_2 of weight 2. Under $(x + ty, y)$, a_0, b_0, d are unaltered so that each Ω_i is unchanged. To complete this direct verification of the invariance of Ω_i, it remains to test the transformation $(y, -x)$. The following special forms of the Ω_i are obviously unaltered by the substitution S which interchanges a_0 and a_2, b_0 and b_2, and changes the signs of a_1, b_1. For $p^n = 3$,

$$\Omega_1 = ba_0a_1a_2(a_2 - a_0) + b_1(b_0 - b_2)(a_0a_2 + a_0^2a_2^2 + a_0a_2a_1^2),$$

the product of $1 + a$ by the invariant $ba_1(a_2 - a_0) - ab_1(b_2 - b_0)$;

$$\Omega_2 = \{b(1 - a_1^2) + b_0^2 + b_2^2\}(a_0^2a_2 + a_0a_2^2) + a_0a_1^2a_2(a_0b_2^2 + a_2b_0^2) + a_1b_1(b_0 + b_2)(a_0a_2 - a_0^2a_2^2).$$

For $p^n = 5$, $\Omega_i = a_0a_2\Omega_i'$, where

$$\begin{aligned} \Omega_1' &= bb_1(a_1^2 + 2a_0a_2)(a_2^2 - a_0^2) + bb_2a_1(2a_0^3 + a_2m) - bb_0a_1(2a_2^3 + a_0m) \\ &\qquad + b_1(b_0^2 - b_2^2)(a_0a_2m - 1 - 2a_1^4) \quad [m \equiv a_0a_2 + 2a_1^2], \\ \Omega_2' &= 2bb_1a_1(a_0^2 + a_2^2)(1 - a_0a_2a_1^2) + bb_0t + bb_2t' + b_0^3v + b_2^3v' \\ &\qquad + (b_0^2 + b_2^2)b_1a_1(2a_1^2 - a_0^2a_2^2a_1^2 - a_0^3a_2^3), \\ t &= 2a_2^3(1 - a_1^4) - 2a_0^2a_2(1 + a_1^4) + a_0a_1^2(1 - 2a_0^2a_2^2), \\ v &= a_0^3 - a_0a_2^2(1 - a_1^4) + a_2a_1^2(a_0^2a_2^2 - 2), \end{aligned}$$

t' and v' being derived from t and v by the substitution S.

The classes with $-a$ a not-square are completely characterized by the invariants a, b, θ, Ω_i. Instead of (39), we may employ canonical types with coefficients in the initial field. For the case $-R$ a not-square, let k be a fixed element for which $(k^2 + R)/(4v)$ is a square ρ^2. Then by (43), (36_2), (40_3),

$$f = \pm\rho, \quad e = (k - \theta)/(2v), \quad g = (k + \theta)/2. \tag{53}$$

Hence any pair of forms with $-a$ and $-R$ not-squares is equivalent under G_1 with one of the two pairs (35), subject to (53). In view of (45_1), the sign of f is determined by the invariant Ω_1.

For $-R$ a non-vanishing square m^2, there occur types (35) with $f = 0$, in view of (43). For such a type,

$$f = 0, \quad e = (-\theta \mp m)/(2v), \quad g = (\theta \mp m)/2 \quad (m = \sqrt{-R}). \tag{54}$$

If an automorph T of $x^2 - \nu y^2$ replaces $ex^2 + gy^2$ by a form lacking xy, then T is either $(\pm x, \pm y)$ or $(\nu\gamma y, \gamma x)$, where $\gamma^2\nu = -1$. Hence the two types (35), with the specification (54), are not equivalent under G_1, if -1 is a square, and may be taken as representatives of the two classes with the invariants $a = -\nu, b, \theta$. Now $\Omega_2 = 2(\mp m)^j$, so that Ω_2 determines $\mp m$, since j is here odd. But if -1 is a not-square, the two preceding types are equivalent; we then employ

$$\pm (x^2 - \nu y^2), \quad \tfrac{1}{2}(\mp\theta + m)\nu^{-1}x^2 + \tfrac{1}{2}(\pm\theta + m)y^2, \tag{55}$$

m being a fixed square root of $-R$. The two types (55) are not equivalent under G_1 when -1 is a not-square. The only transformations of determinant unity which multiply $x^2 - \nu y^2$ by -1 are

$$\begin{pmatrix} \alpha, & -\nu\gamma \\ \gamma, & -\alpha \end{pmatrix}, \quad \alpha^2 - \nu\gamma^2 = -1, \tag{56}$$

viz., transformations (50) on the original variables. If (56) replaces (55_2), by a form lacking xy, then $m\alpha\gamma = 0$, whereas $\alpha \neq 0$, $\gamma \neq 0$, -1 and ν being not-squares. For (55), $\Omega_2 = \pm 2m^j$. Now j is even. Hence Ω_2 differentiates the two types.

THEOREM. *As a fundamental system of invariants of a pair of binary quadratic forms in the* $GF[p^n]$, $p > 2$, *we may take**

$$a,\ b,\ \theta,\ Q_a,\ Q_b,\ K_1,\ K_\tau,\ V_a,\ V_b,\ \Omega_1,\ \Omega_2. \tag{57}$$

17. To determine a complete set of linearly independent invariants, we employ the method of § 6. The invariants in any line of the table are linearly independent, equal in number to the classes in that line, and vanish for the classes in the later lines.

CLASSES.	INVARIANTS.	NUMBER.
$-a$, $-R$ not-squares	$a^s R^\sigma \theta^i \Omega_1$, $[(-a)^\tau - 1][(-R)^\tau - 1] a^{s+1} R^{\sigma+1} \theta^i$	$2\tau^2 p^n$
$-R$ a square, $-a$ not	$a^s R^\sigma \theta^i \Omega_2$, $[(-a)^\tau - 1] a^{s+1} R^{\sigma+1} \theta^i$	$2\tau^2 p^n$
$-a$ not-square, $R = 0$	$[(-a)^\tau - 1] a^{s+1} \theta^i$	τp^n
$-a$ = square	$a^{s+1}\theta^i (b^r,\ b^t K_\tau,\ b^t V_a,\ K_\tau^2,\ K_\tau V_a)$	$\tau p^n (2p^n +$
(34_1)	$b^i \theta^q Q_a^e$	$4\tau p^n$
(34_2)	$b^{s+1} Q_a^e$, $b^{s+1} Q_a^e V_b$	4τ
(34_3)	$Q_a^e K_1^i$	$2p^n$
$q_1 \equiv 0$	b^q, Q_b^e, 1	$p^n + 2$

* In place of Ω_2, we may employ $K_{2\tau}$ and K_1 (in differentiating the classes at the end of this section). Cf. *A. J.*, § 10.

The exponents take independently the following values:

$$s, \sigma = 0, 1, .., \tau - 1; \; t = 0, 1, .., \tau; \; i, r = 0, 1, .., 2\tau; \; q = 1, .., 2\tau; \; e = 1, 2.$$

The total number of linearly independent invariants is thus

$$2p^{3n} + p^{2n} + 2p^n.$$

Obvious linear combinations of those in the table give a simpler set.

Binary Quadratic and Linear Form in the $GF[p^n]$, $p > 2$.

18. Consider the pair of forms

$$q = a_0x^2 + 2a_1xy + a_2y^2, \quad l = rx + sy. \tag{58}$$

In addition to the invariants in § 12, we have

$$R = a_0s^2 - 2a_1sr + a_2r^2, \quad J = (1 - r^\mu)(1 - s^\mu), \tag{59}$$

where R is the resultant of the pair (58) and $\mu = p^n - 1$.

We construct an absolute invariant V with the value α when $q \equiv \alpha l^2$, $l \not\equiv 0$, and with the value zero in the remaining cases. Thus

$$V = v(1 - R^\mu)(1 - a^\mu), \quad a \equiv |q|.$$

To determine v consider the pairs (58) with $R = a = 0$; then

$$q \equiv \alpha l^2, \quad a_0 = \alpha r^2, \quad a_1 = \alpha rs, \quad a_2 = \alpha s^2. \tag{60}$$

First, take $r \not\equiv 0$. Then $v = a_0/r^2$. Hence for any r,

$$v \equiv a_0r^{\mu-2} + k(1 - r^\mu).$$

Next, take $r = 0$, $s \not\equiv 0$. Then $v = a_2/s^2 = k$. Thus, for any s,

$$k = a_2s^{\mu-2} + c(1 - s^\mu).$$

For $r = s = 0$, $v = 0$ by definition. Hence $c = 0$. Thus

$$V = (1 - R^\mu)(1 - a^\mu)\{a_0r^{\mu-2} + a_2s^{\mu-2}(1 - r^\mu)\}. \tag{61}$$

Finally, we shall need an invariant K with the value β when

$$q = 2\beta ll_1, \quad l_1 = \gamma x + \delta y, \quad r\delta - s\gamma = 1, \quad \beta \not\equiv 0, \tag{62}$$

and with the value zero when q is not the product of two distinct linear factors one of which is $l \not\equiv 0$. Thus $K = \varkappa(1 - R^\mu)$. To determine $\varkappa$, consider the pairs (58) with $R = 0$, $l \not\equiv 0$, q/l^2 not a constant. Then (62) holds, whence

$$a_0 = 2\beta r\gamma, \quad a_1 = \beta(r\delta + s\gamma), \quad a_2 = 2\beta s\delta. \tag{63}$$

First, take $r \neq 0$. Then by (62_3) and (63_2), $a_1 = \beta(2s\gamma + 1)$. Eliminating γ by (63_1), we get $\beta = a_1 - a_0 s/r$. Hence, for every r,

$$x = a_1 - a_0 s r^{\mu-1} + m(1 - r^\mu).$$

Next, take $r = 0$, $s \neq 0$. Then $s\gamma = -1$, $\beta s\gamma = a_1$. Thus

$$x = \beta = -a_1, \quad x = a_1 + m.$$

Thus, for every s, $m = -2a_1 + d(1 - s^\mu)$. Finally, take $r = s = 0$, so that $x = 0$ by definition; while $x = -a_1 + d$. Hence $d = a_1$,

$$K = (1 - R^\mu)\{a_1 r^\mu - a_0 s r^{\mu-1} - a_1 s^\mu (1 - r^\mu)\}. \tag{64}$$

It remains to test the pairs for which (60) holds; but the second factor in (64) then vanishes. Hence K is an invariant of weight 1.

We may now characterize invariantively a complete set of canonical types, under the group G_1, of pairs of forms (58).

$$\begin{array}{ll} J = 0, \ R \neq 0: & x, \ R^{-1}ax^2 + Ry^2. \\ J = R = 0, \ a \neq 0: & x, \ 2Kxy. \\ J = R = a = 0: & x, \ Vx^2. \end{array}$$

For $J=1$, then, $l \equiv 0$ and the types (20) for q are characterized by a and Q (§ 12).

Hence J, R, a, Q, K, V form a fundamental system of invariants. As a complete set of linearly independent invariants we may take

$$1, \ J, \ Q, \ Q^2, \ R^i, \ a^i, \ R^i a^j, \ K^i, \ V^i \quad (i, j = 1, \ldots, \mu). \tag{65}$$

Any product of the invariants (65) can be expressed as a linear function of them by means of the following relations:

$$J^2 = J, \ JQ = Q - V^{\mu/2} + R^{\mu/2}(a^\mu - 1), \ JR = JK = JV = 0,$$
$$Ja = a(1 - R^\mu) + K^2, \ Q^3 = Q, \ Qa = 0, \ QR = (1 - a^\mu)R^{1+\mu/2}, \ QK = 0,$$
$$QV = V^{1+\mu/2}, \ RK = RV = aV = KV = 0, \ aK = -K^3, \ t^{\mu+1} = t \ (t = R, a, K, V).$$

Defining the invariant I by (22), we have

$$(1 - I)(1 - J) = R^\mu + K^\mu + V^\mu.$$

THE UNIVERSITY OF CHICAGO, *January*, 1909.